

Abstract of the Disclosure

A method for provisioning a device such as a token. The device issues a certificate request to a Certification Authority. The request includes a public cryptographic key uniquely associated with the device. The Certification Authority generates a symmetric cryptographic key for the device, encrypts it using the public key, and creates a digital certificate that contains the encrypted symmetric key as an attribute. The Certification Authority sends the digital certificate to the device, which decrypts the symmetric key using the device's private key, and stores the decrypted symmetric key.